7 • Additional Comments

Review of Problem and Participants

The fundamental problem presented to PBX owners is control of sneak paths through the PBX that can be exploited for fraudulent use of the long distance public network. The incentive to handle this problem is the interexchange carrier practice, established through tariffs, of charging the PBX owner for all fraudulent long distance calls. The burden of this fraud can be quite large, even devastating to some businesses, and has been the subject of protests to the Federal Communications Commission and others. Seemingly, since it takes the cooperation of many parties to establish a successful telephone service that benefits all, these same parties must cooperate in solutions to the problem at hand, or they will all lose. These parties are the client, the PBX owner, the PBX technical service agency, the PBX manufacturer, the local network carrier, and the long distance network carrier. The technical service agency is usually vertically integrated in one organization with the PBX vendor and the manufacturer, but may be an independent contractor or a part of the owner's organization.

All proposed solutions face a normal constraint: the cost of effective solutions must make good business sense relative to the risks. Some solutions that have been offered, the "fraud insurance" proposals of the interexchange carriers is an example, fail to meet this test for many PBX owners. The cost picture of small PBX systems, those with less than 100 station lines, is especially sensitive to added burdens and great care must be taken in developing solutions for them.

Service Agency Relationship

This paper has described an approach that may be taken by PBX owners. This may be summarized as three major steps: secure the PBX, close any sneak paths that may be exploited for toll fraud, and check or monitor the results. This approach has its costs and novel aspects that may not be practical in all ways, and all cases. The success of the approach is highly dependant on the relationships between the PBX owner and the service agency.

While the owner always has responsibility for the proper use of the PBX system, the key party in preventing or controlling PBX-based toll fraud is the technical services agency employed to install and maintain the system. The PBX owner is very dependant on their skill and knowledge of the system, the quality of their service concepts and their ability to manage technical services. PBX manufacturers, vendors, and their service contractors have established a protected position that shields them from the consequences of their errors. The standard service contract typically has a waiver of consequential damages that was intended to protect the contractor from the owner's loss during equipment failure. In practice this gets extended to include installation errors that result in sneak paths or vulnerability to hacking. It would be unusual for the PBX owner

to have enough market power to negotiate significant changes to the offered contract. Once the PBX has been acquired, the owner, for most practical purposes, has lost the option of taking the business elsewhere. Considering the vulnerability of the owner, some redress of the situation is in order, perhaps through legislation.

Traffic and CDR Monitoring

Monitoring of the PBX system has been described as the third major step the PBX owner can take. A cost-effective way is to add traffic monitoring and CDR screening to an intelligent alarm system that exists for system reliability purposes. The process is to monitor an information stream that contains alarm information, filter for the alarm conditions of interest and report these to a full-time network management center. The new items would be to monitor PBX traffic and screen it against a profile, and to monitor the CDR stream for suspicious calls such as calls to the 809 area. If the filters are good enough, alarms will be raised when fraud takes place and a technician can be called to examine the PBX. This kind of alarm equipment can add ten percent to the investment in small PBX systems, plus the alarm system operating costs. If the PBX service agency does not support centralized alarm monitoring, the owner may have to acquire a complete system and enlist a burglar alarm monitoring company to watch it.

Monitoring By Interexchange Carriers

This paper outlines one systematic approach that PBX owners can follow to control toll fraud. It has its costs and, unless the service agency has the skill to take a highly-disciplined approach, the results will be uncertain.

There is a need to assess the toll fraud monitoring capabilities of the interexchange carriers as part of the search for a workable and acceptable toll fraud control method. The capabilities and nature of the carriers' systems are not widely known. Clients and regulators cannot reasonably conclude whether such monitoring is doable and, if so, how the costs should be borne. What can be said is that unlike calling card fraud, incentives for carriers to address PBX-based toll fraud in a fair manner do not exist. With the current lack of regulation the carriers are not at all at risk, only the clients are at risk.

One way an Interexchange carrier monitoring system might work would be to establish an agreed customer profile of normal calling, monitor calls on a near real time basis, keep a running total of the various call types, reject calls that exceed the profile thresholds, and immediately consult with the customer when rejection occurs. Superficially at least, this is like the process the carriers use for calling card fraud control.

A separate but related issue that must be addressed is the carriers current practice of recovering both their costs and "profits" when PBX-based toll fraud occurs, i.e., charging of full rates.

In summary, the present fraud insurance offerings of the carriers are not good enough. Corrective action at the PBX may not prove sufficient.

This page intentionally left blank.

8 • PBX Toll Fraud Examples

Introduction

Following are examples of toll fraud. Contributing factors in many instances were weak procedures by the service agency and/or flawed designs by the manufacturer. In one instance a manufacturer developed their version of through-dial to their Voice Mail system as a standard feature and configured the feature initial condition so that the feature was turned on and a sneak path established unless action was taken to disable it. This made any equipped PBX immediately vulnerable to hacking. Hindsight shows this to have been an imprudent response to the demands of some clients. Details of the following examples may not be exact since a precise technical understanding of these kinds of events is always difficult.

Voice Mail Through-Dial and PBX Hacking

A new PBX was established with Voice Mail through-dial included as a feature in the vendor's package. Clients, upon hearing of the feature, demanded it as a means to provide better service to their customers, despite advice of their Corporate telecoms agency. The feature was discovered and exploited by the fraud community, and was removed from service. Later, during a PBX software upgrade, the PBX central processing unit remote access password (PBX password) came to be set to the manufacturer's widely known default condition and was not reset to the proper password by the service contractor. This was quickly discovered by a hacker who reestablished the through-dial feature for the fraud community. Losses during the second event may have been $10,000.

Renegade Technician

A renegade technician working for a service agency in a large metropolitan area made a business of establishing sneak paths in PBX's under his care, selling information on the sneak paths to toll fraud operators, and then closing the path to avoid detection. This was repeated many times.

Through-Dial and Toll Restrictions

A PBX was established with Voice Mail, including the through-dial feature. A hacker penetrated some mail boxes and was able to gain switched access into the PBX. The hacker explored the PBX and found a path to the outside that was not adequately guarded by toll restriction and was able to gain access to an international operator. The operator was coaxed into manually placing calls by the calling parties who claimed they had trouble dialing direct. The operator called the unusual volume of calls to the attention of the IXC's security unit.

Overall about two weeks went by before inquiries were made of the PBX owner and the sneak paths were found and closed. Loss was in excess of $100,000.

Through-Dial and PBX Hacking

A PBX had 800 service associated with several station lines, the lines were forwarded to a Voice Mail with through-dial. The PBX became subject to toll fraud, and was cleaned up with the through-dial option toll restricted to keep calls within the PBX. The PBX remote access port was protected by a four-character password (the manufacturer's maximum at the time). A feature to temporarily lockout remote access after unsuccessful logon attempts was equipped but not set. The PBX was also equipped with an advanced form of automatic route selection (ARS). Later the PBX was successfully hacked. The hacker established a sneak path by specifying a station number as an ARS access code that would forward a call coming from the voice mail system to a central office trunk and auto-dial an IXC access code. The fraudulent process then became: dial the 800 number into the PBX, wait for transfer to voice mail, dial the through-dial access code and the new ARS access code followed by a number in the 809 area. The calls were not logged by the PBX CDR system. Loss during the second event was thought to be about $10,000.

Default Passwords

A PBX was equipped with Voice Mail, including through-dial. The through-dial access was protected by a password; however, the password was left at the manufacturer's initial setting by the service agency. A hacker was able to penetrate mail boxes and the through-dial access and found a suitable long distance access method via the owner's private virtual network. Loss was estimated as $10,000 minimum.

Third-Party Billing

A PBX was jointly used by several corporate clients. The long distance charges were screened for totals, but otherwise not carefully scrutinized. That third-party charges against the PBX listed directory number would be accepted by the local telephone company (i.e., not verified with the customer) became known by a segment of the local community. Verbal orders against accepting third-party charges had been given to the telephone company. Third-party fraud became established at a modest level and grew over a period of years. Some participants began making international calls, raising the fraud to a level that was noticed. Written orders were finally issued to the local telephone company to institute automatic denial of third-party billing. Losses were estimated at roughly $12,000 per month at the time of discovery.

Disgruntled Employees

A technician working for a service agency became "at odds" with a PBX owner. Sometime later an employee of the owner noticed an unusual crowd around a nearby telephone booth. The technician had written a voicemail password and instructions on how to make free long distance calls on the wall of the booth. Loss was estimated at $15,000.

This page intentionally left blank.

9 • PBX Toll Fraud Prevention Checklist

Introduction

This section presents three examples of PBX Toll Fraud Prevention Checklists. Although the examples may have been written with one or two types of PBXs in mind, they are general enough to serve as guides for other types of PBXs. While checklists cannot guarantee 100% protection from toll fraud, they do suggest effective steps that can be taken to discourage unauthorized persons from breaking into the PBX.

Example 1 PBX Toll Fraud Prevention Checklist

Physical Security

Control Objective

Adequate physical security should exist to prevent unauthorized conversion of company assets and any breach of sensitive information.

1. Ensure all telephone circuits in use for voice communications are adequately secured.
2. Determine if the voice communications processing equipment is located in a physically secured area.
3. Evaluate the fire suppression system protecting the voice communications equipment.
4. Evaluate security over the switchboard operator's telephone consoles.
5. Perform relevant tests in the small scale computer center audit program.
6. Review the maintenance vendor check-in procedures. Does the vendor register with the offices' receptionist?

Inward PBX Access

Control Objective

Adequate system security precautions should exist over inward PBX access to prevent unauthorized conversion of company assets and any breach of security.

1. Document all inward PBX access points (e.g., trunks, direct dial, 800 service).
2. Review security over all inward 800 services.
   a. Is the access point adequately secured with barrier and authorization codes?
   b. Verify that the 800 number is unpublished and confidential.
   c. Ensure adequate area code blockages are installed to prevent incoming calls from non-business locations.
3. Ensure all maintenance and programming ports are protected with multiple passwords. Verify that their passwords are changed on a frequent basis.
4. Review local switchboard operator procedures. Verify that inbound callers are not transferred to an outbound trunk line.

5. Document the usage of all Direct Inward System Access (DISA) extensions. Verify that there is a legitimate business purpose for the extension. (These extensions provide a hacker an prime access point into the PBX system.)

   a. Verify that the password is at least 8 characters in length.

   b. Verify that the passwords are changed frequently (i.e., at least weekly).

Outbound Long-Distance Service

Control Objective

Adequate system security precautions should exist over outbound access to prevent unauthorized conversion of company assets and any breach of security.

1. Ensure access is restricted against area codes 900, 905 (Mexico), and 809 (Caribbean Islands). Ensure access is restricted to exchange 976. Attempt to make phone calls using these numbers: (1-900-555-5555).

2. Verify that access to the outbound trunk lines (local and long-distance) are restricted for callers on company's communication network.

3. Verify that the PBX is programmed to restrict international calls to only those countries that are necessary.

4. Verify that conference room telephones are restricted from local and long-distance dialing.

5. Review remaining restrictions to outside local (i.e., radio stations, local stockbrokers, time, and temperature) and long-distance trunk lines for appropriateness.

6. Ensure the system is prevented from external call forwarding by attempting to call forward to an external number.

7. Review client extensions with "unrestricted" network class of service (NCOS) and/or "unrestricted" trunk group access restrictions (TGAR) for appropriateness. Also, review consoles which are "maintenance allowed" (MTA) and operator.

8. Review security over the system's maintenance lines. Ensure a caller cannot obtain an outside line by dialing these maintenance lines.

Voice Mail/ Automated Attendants

Control Objective

Adequate system security precautions should exist over the voice mail system and automated attendants to prevent unauthorized conversion of company assets and any breach of security.

1. Verify that all outbound trunk access codes and miscellaneous numbers are restricted to prohibit outdialing through both the outbound trunk and T-1 lines.

2. Verify restrictions on all thru-dial menus and automated attendants to prevent outdialing through both outbound trunk and T-1 lines.

3. Verify restrictions to any voice response system to prevent access to the PBX.

4. Verify that voice mailboxes are disabled after 3 invalid sign-on attempts.

5. Ensure client mailboxes are password protected. Verify that the voicemail PC and administrator account passwords are changed frequently.

6. Verify that the voice mail modem and communications hardware are adequately controlled.

Security Reporting

Control Objective

Security features in the network should provide an adequate audit trail of network activity, and alert management to potential security violations.

1. Determine whether the network is equipped with activity logging and error reports. Ensure the reports are reviewed on a regular basis.

    a. Review reports for any unusual length calls particularly to international locations.

2. Ensure that network security violations are reported to management.

Example 2 PBX Toll Fraud Prevention Checklist

Site: _____ Audit by: _____
Regional Supervisor: _____ Date of Audit: _____

	Action	Completed	Date	Initial
1	**Physical Access:**			
	a) Switchroom door access controlled.			
	b) All common telephone room/closets access controlled.			
	*Note: If CTD has no control over the room, then building management needs to address the security issue.			
2	**Long-Distance Restrictions:**			
	a) Common area phones restricted from Long-Distance dialing (as required).			
	b) Time of Day (TOD) control implemented as required.			
	c) Area codes (809 and overseas call) access restricted; allow only as required.			
	d) International Direct Dialing (IDDD...011) restricted; allow only as required.			
3	**Client's Awareness on Toll Fraud:**			
	a) ACD operators/agents trained.			
	b) Attendants trained.			
	c) 800's number owners trained.			
	d) All CTD employees trained.			
4	**DISA:**			
	a) All Direct Inward System Access (DISA) removed/disabled.			
5	**Dial-in PBX Maintenance Port:**			
	a) Password changed quarterly.			
	b) Minimum password should be 8 digits alpha-numeric: (random)			
	i) 8 digits alpha-numeric (if release 16 is available/feasible to upgrade).			
	ii) If switch has only 4 digits password, then change password every month.			
	iii) Change password immediately after cutover (if applicable). (No default password)			
	c) Recommend using maintenance modem with dial back capability; change default password.			
	d) Has Site Event Buffer (SEB) been installed?			
	e) Program OVL15 error message into SEB to be reported as a major alarm.			

	Action	Completed	Date	Initial
	"Note OVL15 is Northern's error message for "Password is incorrect."			
	f) If switch has release 16+ software, then limit the number of invalid password attempts to five or less.			
6	**Dial-in Voice Mail Maintenance Port:**			
	a) Password changed quarterly.			
	b) Minimum password should be 8 digits alpha-numeric: (random)			
	i) 8 digits alpha-numeric			
	ii) If voice mail has only 4 digits password, then change password every month.			
	iii) Change password immediately after cutover (if applicable). (No default password)			
	c) Recommend using maintenance modem that has dial back capability; change default.			
7	**Software/Features:**			
	PBX			
	a) Ensure that only one remote access TTY port programmed.			
	b) Verify all steering codes for validity.			
	c) Deny all external forwarding.			
	d) If external forwarding is needed, then deny forwarding to the following:			
	i) 8			
	ii) 9			
	iii) 9+1, 9+0, 9+00			
	iv) 8+1, 8+0, 8+00			
	v) Allow call forward to a maximum of 8 digits.			
	vi) Deny trunk to trunk access:			
	1) DID should not access COT.			
	2) SDN should not access COT.			
	vii) Deny all call forward to trunk access codes.			
	viii) Deny call forward to 900, 976, and 700 (allow only if required).			
	e) Deny radio contest prefixes.			
	Voice Mail			
	a) Clean up all Voice Mail databases:			
	i) Remove all default mailboxes.			
	ii) Remove all invalid mailboxes.			
	iii) Remove all unused mailboxes.			

	Action	Completed	Date	Initial
	b) Thru-dial:			
	i) Restrict thru-dial to extension only.			
	ii) Restrict thru-dial to all leading digits except extension digits and revert number.			
	c) Remote notification should be enabled for authorized users only.			
	d) Voice Menu:			
	i) Make client aware of the consequences of using voice menu to automatically dial an external number.			
	ii) Do not allow voice menu to forward to 8 or 9.			
	e) Set forced password change to 90 days (recommended).			
	f) Restrict Voice Mail Virtual Agents with low FRL (facility restriction level).			
8	**CDR:**			
	a) Is CDR (Call Detail Recording) set to provide alarm for "toll fraud area codes?" (i.e., 809-Puerto Rico; 505-Nicaragua; 504-Honduras; 503-El Salvador; 511, 517-Peru; 593-Ecuador; 571, 572, 574, 576-Columbia; 809-Jamaica)			
9	**Documentation:**			
	a) Secure all NTPs, manuals, and instructions from public access.			
	b) Discard all switch print out properly (e.g., shred the materials).			
	c) Password should not be visible to the public.			
10	**Modem Pool:**			
	a) Invoke maximum password on modem pool.			
	b) Do not allow inbound modem trunk to be able to call out on outbound modem.			
	c) Do not allow inbound modem trunk to be able to access voice mail, extensions.			
11	**Central Office and Long-Distance Carriers:**			
	a) Make sure that modem numbers and maintenance port numbers are unpublished.			
	b) Make sure that "third-party billing" is blocked for site.			
	c) Make sure that area code 809 is blocked by LEC/AT&T for site that does not need it.			